Remarks

In the application, claims 1 through 15 are pending. No claims currently stand allowed.

The Office Action dated January 13, 2005, has been carefully considered. The Office Action rejects claims 1 through 15 under 35 U.S.C. § 103(a) as obvious in light of U.S. Patents 6,311,218 ("Jain"), 5,684,951 ("Goldman"), and 6,052,788 ("Wesinger").

The present application describes a user-authentication scheme that is "out-of-band," that is to say, that is outside of the protocols used to transmit "network" data. ("Network" data means data that are not transmitted solely as part of the user-authentication scheme.) The user authenticates himself via a public/private encryption key-based, challenge/response mechanism. However, because this authentication scheme is out-of-band, the existing data transmission protocol cannot make use of the authentication. Therefore, there needs to be some way to associate the authenticated user with the network data actually transmitted by the user. The present invention solves this by encrypting a portion of the user's transmitted network data into a "message digest" and by then making the encrypted message digest part of the authentication process. Only the authenticated user has the knowledge needed to correctly perform this encryption. The policy agent that performs the authentication compares the network data transmitted by the user with the message digest, which it can decrypt. If they match, then the policy agent knows that these network data must have been transmitted by the authenticated user.

The network data are thus *used* in the authentication scheme of the present invention, but they do not exist *solely* as part of the authentication scheme. The user transmits them primarily in order to perform some network task other than authentication (to query a database or to retrieve a web page, for example). Once the network data are associated with an authenticated user, the policy agent can decide whether to accept them for their non-authentication purpose (probably by passing them on to their intended recipient, see the specification, page 4, lines 4 through 5, and page 10, lines 8 through 13 and lines 21 through 23). Network data that cannot be associated with an authenticated user can be rejected (for example, see the specification, page 14, lines 15 through 24).

In a manner somewhat similar to the present invention, Jain describes a user-authentication scheme based on a public/private encryption key, challenge/response mechanism. However, Jain's authentication mechanism is entirely *in-band*, so that it does not need to address the problem of associating in-band network data with an out-of-band user-authentication. Applicants disagree with the Office Action that Goldman and Wesinger make up for this lack in Jain. While the cited art discusses the role of user data in the authentication process (of course), nowhere in the cited art is there a discussion of the use of that *same* data for some purpose beyond user authentication. Neither Jain, Goldman, nor Wesinger, either separately or in any combination, anticipates or renders obvious the following combination of elements of claim 1:

> Claim 1: *receiving network data through the network connection with the client computer;*
>
> *calculating a second message digest value based on the challenge and the received network data;*
>
> comparing the first and second message digest values to determine whether a match is found; and
>
> *if a match is found, then forwarding the network data to their specified recipient,* else not forwarding the network data to their specified recipient.

(Emphasis added.) (Claim 8 has similar language.) In the portion of Goldman cited by the Office Action for "a second message digest value based on . . . the received network data," the "received network data" is found in Goldman's "secret code." This is an invalid reading, however. Goldman's secret code is used *solely* for authentication, and nowhere does Goldman discuss forwarding the "secret code" to its specified recipient, after a match is found, as is required of the network data in Claim 1. Therefore, Goldman's secret code does not anticipate the network data of claim 1.

Similarly, the first cited section of Wesinger (column 4, lines 1 through 5) discusses sending an "access key" which is used *solely* for authentication and is thus not Claim 1's network data. The other cited section of Wesinger reads as follows:

> The different virtual hosts may also be configured to perform channel processing of various sorts as traffic traverses different network segments. Channel processing may include encryption, decryption, compression, decompression, image or sound enhancement, content filtering, etc. Channel processing is the processing performed on data flowing through a communications channel to enhance some attribute of the data, such as security, reproduction quality, etc.

Wesinger, column 10, lines 58 through 66. Clearly, this section does not discuss the use of the data sent for a non-authentication purpose also *being used in an authentication scheme*. In sum, the cited art simply does not show the combination of claim 1 elements quoted above.

As the combination of the cited art neither anticipates nor renders obvious these independent claims 1 and 8, and as all other currently pending claims depend from these two claims, applicants request that the rejections be withdrawn and that all currently pending claims be allowed.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

John Bretscher

John T. Bretscher, Reg. No. 52,651
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312)616-5600 (telephone)
(312)616-5700 (facsimile)

Date: March 1, 2005